Fault Injection Attacks

Attack Methodologies, Injection Techniques and Protection Mechanisms

Shivam Bhasin and Debdeep Mukhopadhyay

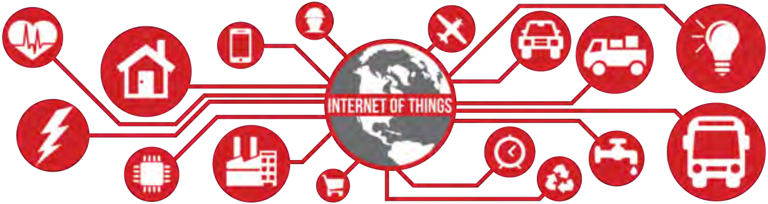
Temasek Laboratories, NTU Singapore
IIT Kharagpur, India
ESP-Research, India

SPACE 2016 – Invited Tutorial
Hyderabad, India. 15 December 2016

Tutorial organization

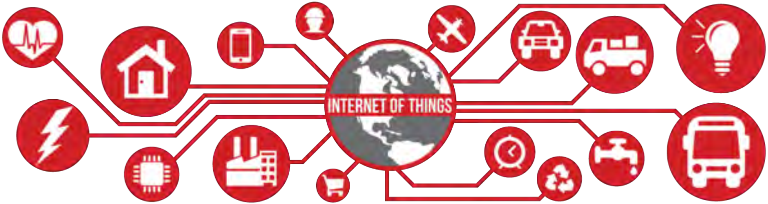
- Part I: Practical Aspects
  - Background
  - Injection techniques
  - Protection Methods
- Part II: Theoretical Analysis
  - Brief History
  - Differential Fault Analysis
  - Biased Fault & Countermeasures
  - Fault Tolerance

Internet of Things



Source: http://ariasystems.com

Internet of Things



IoT Trends

- Population: 4.9 Billion (2015) to 25 Billion (2020)
- Market: $69.5 Billion (2015) to $263 Billion (2020)

Source: Gartner, Inc., Nov 2014

Source: http://ariasystems.com

Internet of Things

Critical Applications of IoT

- Aerospace.
- Automotive.
- Energy.
- Health Care.
- Transportation.
- ...

Internet of Things

Critical Applications of IoT

- Aerospace.
- Automotive.
- Energy.
- Health Care.
- Transportation.
- ...

Vulnerable Devices

- **Smart devices**: smartcards, tags, IoT sensors;
- **Storage devices**: USB sticks, hard-drives;
- **Security devices**: HSM;
- **Computing devices**: cloud.

Why Should We Care?

Why is Hardware Vulnerable?

- IoT is breaking traditional boundaries and locals.
- Devices are present anywhere and everywhere, outsourced.
- Some deployments are in hostile environments.
- Adversary has physical access.
- Are traditional protection enough?

Common Threats to IoT

Software Attacks

Source: http://img.brothersoft.com/

Common Threats to IoT

Counterfeits

Source: http://www.eeherald.com/images/cfeit.jpg

Common Threats to IoT

Physical Attacks

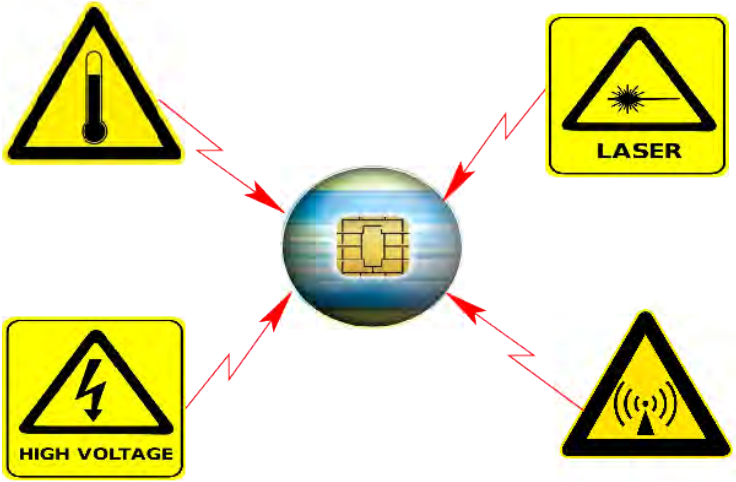
Source: http://www.inmagine.com

Common Threats to IoT

Hardware Trojans

Source: http://computer.org

Fault Injection Attacks (FIA)



Overview of Fault Injection Techniques

Low-Cost and Global

- Power Glitch
- Clock Tampering
- Temperature Variation

High-Cost and Local

- Light/Laser Injection
- EM Injection
- Focused Ion Beam

Impact of Fault Injection

Fault Duration

- Transient
- Harmonic

Fault Effects

- Data Modification
- Flow Modification

Fault Objectives

- Bypass Security Check
- Corrupt Computation
- Bias inputs

Fault Models

- **Single/multiple bit-flip** – a target variable was altered either by single or multiple bit flip.
- **Random byte fault** – Some bits of a byte are flipped. No-precise multi-bit flip.
- **Instruction skip** – One or several instructions were not executed (for software)
- **Stuck-at fault** – target variable stuck at-0/1.

Overview of Fault Protection

Two Approaches:

- Fault Detection
- Fault Prevention

Fault Detections

- Incremental Approach
- Analog Method: Detect physical stress
- Digital Method: Detect modification of digital data

Fault Prevention

- Provable Approach
- Infect/Erase Output

Real World Examples

- Pentium FPU bug attack
  - Bug in Intel P5 floating point unit
  - Outputs wrong result (1 in 9 billion)
  - Shamir proposed attack to retrieve RSA key
  - Can be performed remotely
- PS3 Hack
  - otherOs feature allows boot of Linux
  - Glitch allows hypervisor access
  - Attacker gain full memory access
  - Control of Os bootchain

Fault Injection Techniques

- Widely classified as:
- Global
  - + Low-cost
  - + Applicable on range of devices
  - + Low expertise required
  - - Limited precision
- Local
  - + Precise and powerful
  - + Can bypass basic protections
  - - High expertise required
  - - Expensive equipments

Global Fault Injection: Power

- **Main Idea:** Disturb the power supply to induce faults.
- **Modes:** short-lived glitch, source manipulation
- **Equipment**: Low cost basic lab equipment
- Attacker can feed higher or lower power.
- Potential for remote execution

Global Fault Injection: Power

- Glitches effect are short-lived.
- Are generally used for skipping key instruction
- Timing of the glitch is the key
- Widely used in to tamper payTV cards in 90's
- Typically used to skip watchdog counter or sanity checks
- Power supply can filter some glitches

Global Fault Injection: Power

- Under/Over-powering over prolonged period can also be used for fault injection
- Underpowering increases signal propagation delay
- Can lead to setup time violation in hardware platforms
- In microcontrollers, power hungry instruction are worst hit (memory read/write)
- Overpowering causes electrical anomalies
- Capable of bit-flips

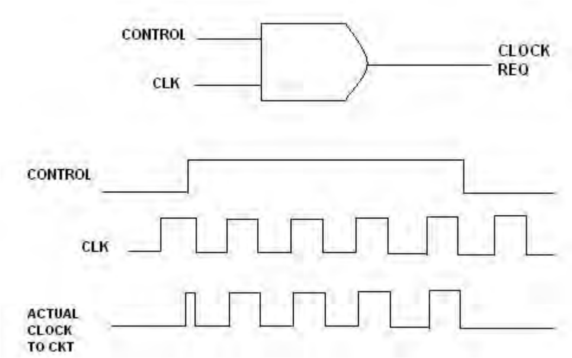
Global Fault Injection: Power

- Recent addition: Body Bias Injection
- Requires access to substrate of the chip (backside)
- A needle is used to inject power directly in the substrate
- Direct access and can bypass glitch detectors
- Powerful but needs basic profiling

Global Fault Injection: Clock

- **Main Idea:** Disturb the clock to induce faults.
- **Modes:** short-lived glitch, source manipulation
- **Equipment**: Low to medium cost equipment
- Overclocking is typically used

Global Fault Injection: Clock



Clock Glitch

Global Fault Injection: Clock

- Clock is a vital resource of electronic circuits
- A clock glitch can be used to reduce period of a one to few operations
- Reduced period leads to wrong computation i.e. fault
- Again timing is the key
- Constant overclocking can inject faults in critical path
- Capable of bit-flips

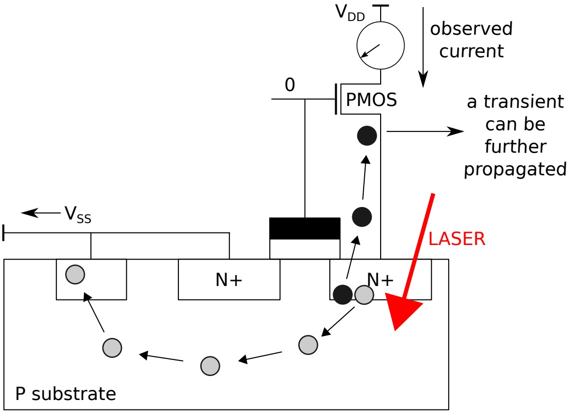
Global Fault Injection: Temperature

- **Main Idea:** Operate in non-nominal conditions
- **Equipment**: Low cost
- Both cold and hot temperature can be used
- Lacks precision

Local Fault Injection: Light

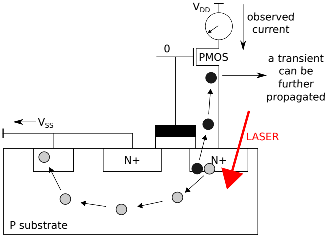
- **Main Idea:** High energy light to induce faults.
- **Modes:** intense flash lamps, laser beam
- **Equipment**: Medium to high cost
- High precision and repeatability
- Needs chip preparation

Local Fault Injection: Light



Impact of Laser on Transistor

Local Fault Injection: Light



- Photoelectric effect - when a laser beam with a wavelength corresponding to an energy level higher than the silicon bandgap passes through silicon, it creates electrons-hole pairs along its path.
- If the laser beam passes through the reverse-biased PN junction of a transistor, charge carriers can be drifted in opposite directions and a current pulse is created. This current pulse creates a transient voltage pulse which propagates through the combinatorial logic of the IC.

Local Fault Injection: Light

- This phenomenon is called a Single Event Transient (SET)
- Fault is induced if a SET propagates through the logic and is captured by a register
- Single Event Upset (SEU) occurs when the transient voltage is directly induced into a SRAM or a register: it flips and locks its state to the opposite one
- It is desired to adjust power for faults but avoiding damages.

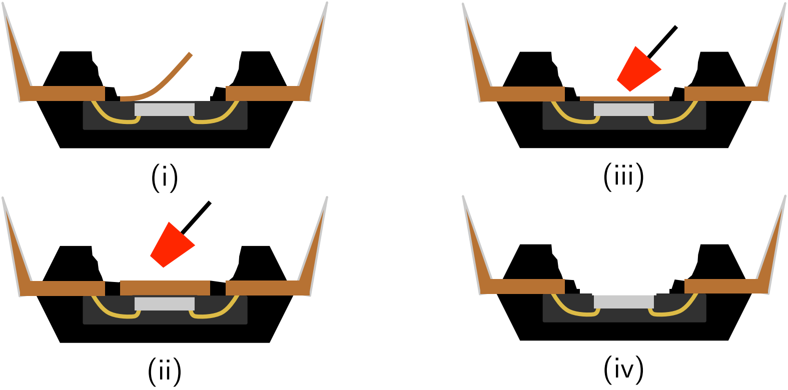
Local Fault Injection: Light

- Laser can be injected from frontside or backside of the chip
- Frontside is more effective with smaller wavelength
- Modern ICs with several metal layers make it less effective
- Backside injection is more suited with near infrared (NIR $\approx$ 1064nm)
- Silicon substrate is transparent to NIR

Decapsulation

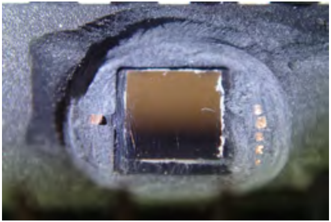
- **Main Idea:** Open the package to access the chip
- **Equipment**: Chemical or Mechanical
- Semi-Invasive Method
- Can be fatal to the chip

Back Side Decapsulation (Mechanical)



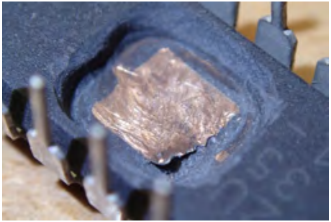
Back Side Decapsulation (Mechanical)

(i)



(ii)

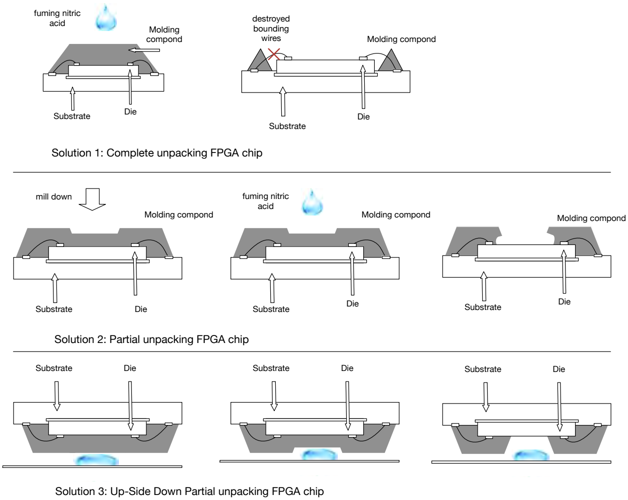
(iii)



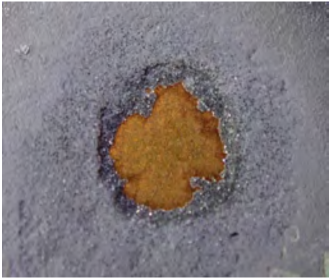
(iv)

Front Side Decapsulation (Chemical)

Front Side Decapsulation (Chemical)



Front Side Decapsulation (Chemical)



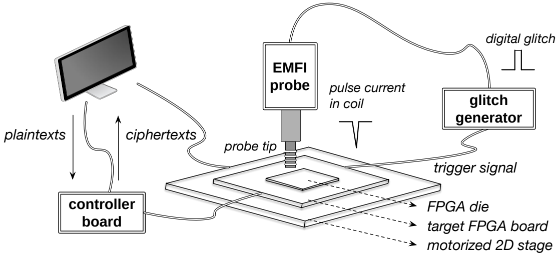
Alive Chip

Broken Chip

Local Fault Injection: Electromagnetic (EM)

- **Main Idea:** High energy EM field to induce faults.
- **Modes:** pulse, harmonics
- **Equipment**: Medium to high cost
- Less precise than laser
- No need of chip preparation

Local Fault Injection: Electromagnetic (EM)



Basic EM Injection Setup

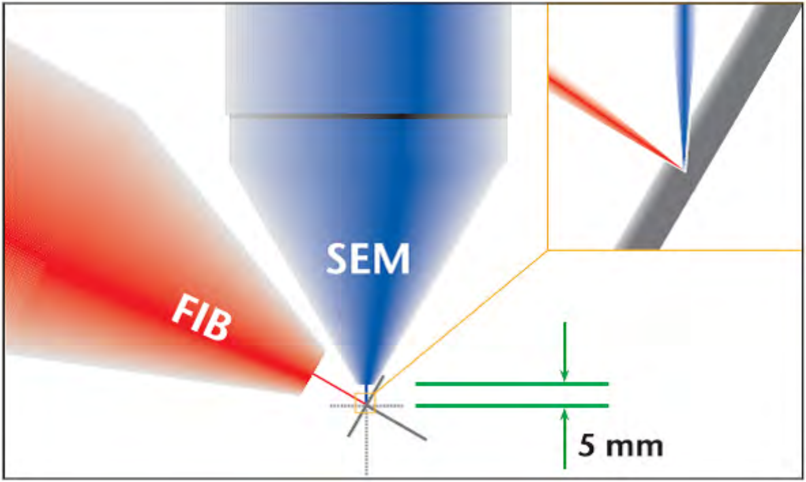
Local Fault Injection: Electromagnetic (EM)

- Low voltage harmonics constantly bias the target
- Generally used for analog blocks like RNG
- Alternatively intense, short pulses can disturb particular operation
- Suited for digital blocks like logic/memories
- Can penetrate several metal layers
- Probe design is a key expertise

Local Fault Injection: Focused Ion Beam (FIB)

- **Main Idea:** High energy ion beam to induce faults.
- **Equipment**: very high cost
- Can make permanent faults
- Very high precision

Local Fault Injection: Focused Ion Beam (FIB)



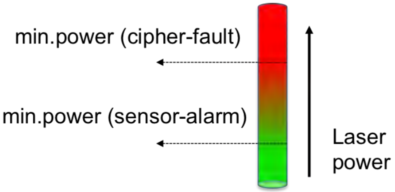
Source: http://mc.missouri.edu

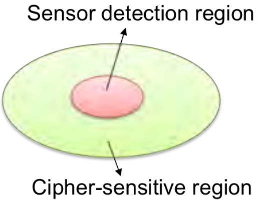
Fault Protection

- Two Approaches:
- Detection
  - Detect injection attempts
  - A recovery mechanism is followed
  - Normally characterised by detection rate
  - Overhead widely varies
  - Information-level methods detect data modification
  - Circuit-level methods perform sanity checks on physical parameters
- Prevention
  - Provable approach
  - Either corrects or infects a fault
  - can have huge overheads
  - Data retrieved by attacker is not exploitable
- A combination of both is often desired

Detector Based Protection

- Eligible sensor/detector should sense physical disturbance
- Desirably independent of the target to contain the overhead
- offer higher senstivity to physical disturbance
- Should react in real-time
- Security margin: Power, Space.



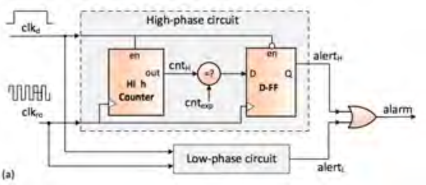


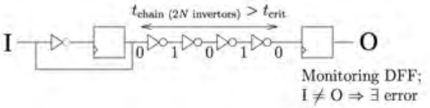
Global Detector

- Glitch on power or clock is a common injection technique
- Analog glitch detectors can be in-built into the IC
- Checks for voltage range, clock frequency etc.
- Out of range operation, triggers recovery.

Global Detector

- Digital detectors can be integrated
- Monitors underpowering or overclocking
- Calibration can be hard and limiting factor
- Also can be used for EM detection





Source: Despande et al. A Configurable and Lightweight Timing Monitor for Fault Attack Detection. ISVLSI 2016

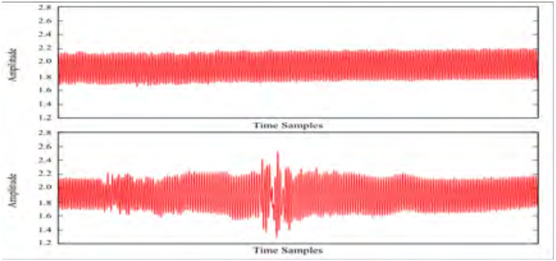
Source: Selmane et al. WDDL is Protected Against Setup Time Violation Attacks. FDTC 2010

Laser Detector

- Laser injects high-energy using an intense beam
- Detailed cartography is required to determine PoI
- Integrated detectors can be deployed to detect laser
- Analog detectors are generally based on photodiodes
- Similar functionality can be detected by custom logic

RO-Based Laser Detector

- Ring oscillator (RO) has tendency to stabilise
- A high-energy by laser will disturb RO oscillations
- This forces RO to loose the lock

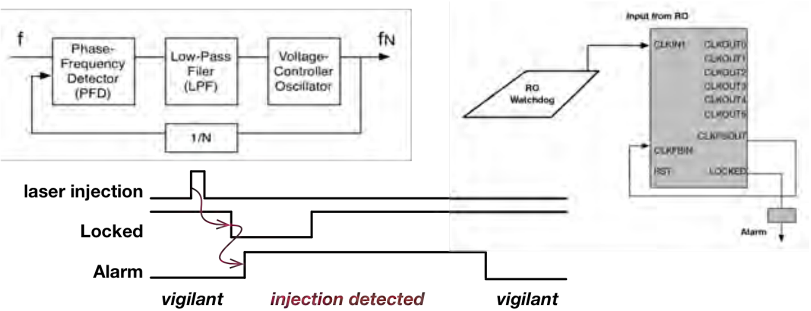


RO Frequency without laser impact

RO Frequency with laser impact

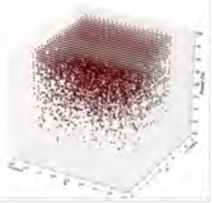
RO-Based Laser Detector

- RO can be used as laser watchdog
- PLL is used to detect the lock
- PLL is a widely used analog component in circuitries for providing stable and precise clock source.
- The lock signal of PLL detects laser injection



RO-Based Laser Detector

- High detection rate
- Offers great power and security margin

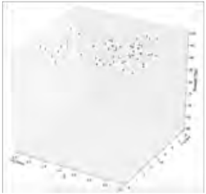


$N_{injected}$	752
$N_{undetected}$	54
$N_{countermeasure}$	5759

Detection Rate: chance to detect the injected faults

$$R_{data} = \frac{N_{injected} - N_{undetected}}{N_{injected}}$$

92.82%



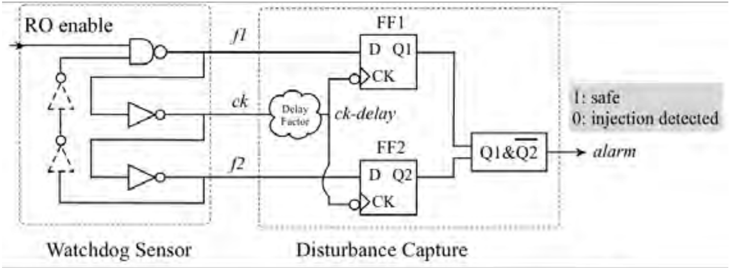
Injection Success Rate: chance to inject faults without triggering alarm

$$R_{undeteced/countermeasure} = \frac{N_{undetected}}{N_{countermeasure}}$$

0.94%

RO-Based Laser Detector

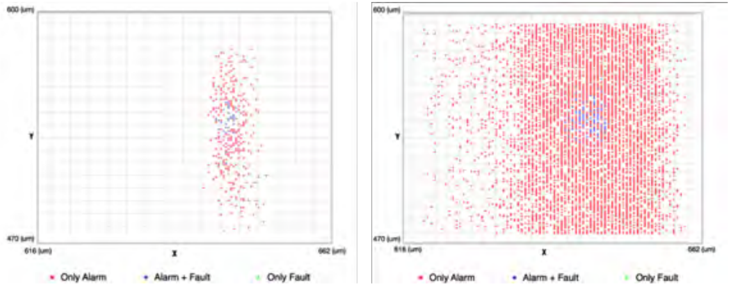
- PLL can be replaced by all-digital logic
- Low-cost, high sensitivity and versatile
- Can also be used to detect glitches



Component	LUT	DFF
Watchdog Sensor	3	0
Disturbance Capture	1	2
Delay	1	0

RO-Based Laser Detector

- PLL can be replaced by all-digital logic
- Low-cost, high sensitivity and versatile
- Can also be used to detect glitches



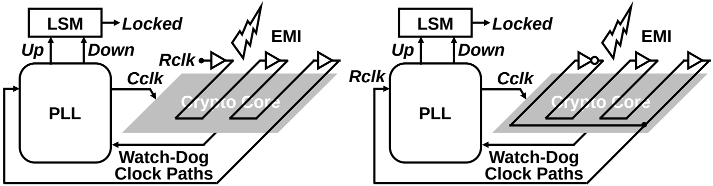
PLL-based Sensor (left) vs All-Digital Sensor (right)

EM Detector

- EM also injects high-energy pulses
- Impact area much larger than laser
- Some solution use local glitch detector for EM
- Recent work [Miura et al.] proposed RO+PLL for EM detection
- Can also replace with digital detector
- Differs in RO routing from laser version

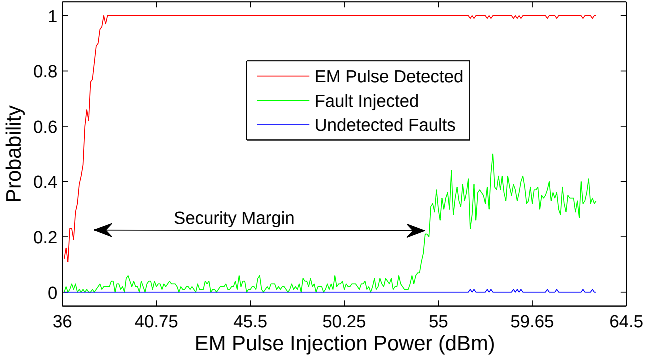
EM Detector

- Security enhanced repeater mode by merging Ref clock with watchdog clock.
- RO-based internal clock to prevent advanced attacks like FSA
- Area Overhead: 1 LUT (RO) + 1 PLL + Routing resources



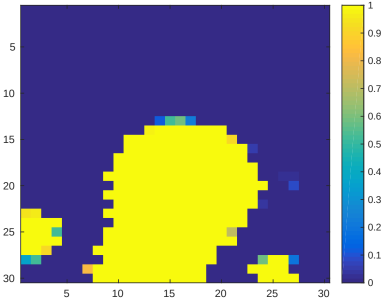
(a) Repeater Configuration (b) Ring-Oscillator (RO) Configuration

EM Detector

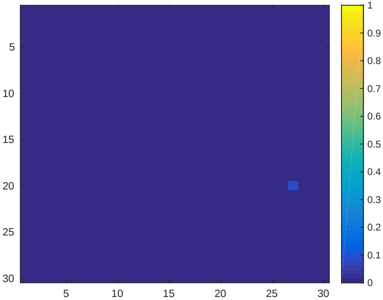


Security Margin = 19dBm

EM Detector



(a) Detection Rate



(b) Undetected Faults

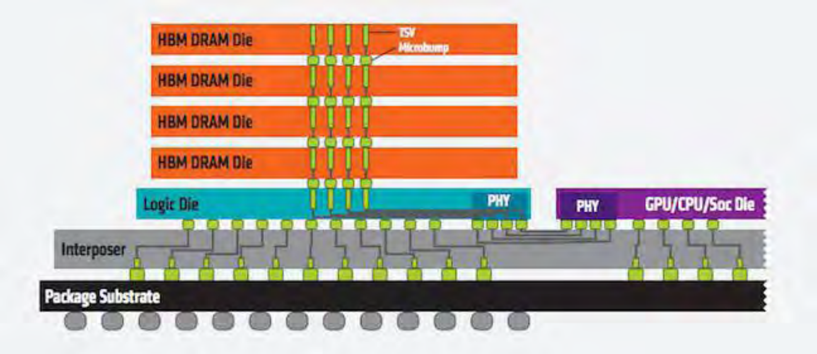
2-D Area Scan (XY axes)

Scan precision $\Rightarrow 1.0\mu m$, Scan Matrix $\Rightarrow 30 \times 30$

Undetected Fault Probability ≤ 0.01

Complex Package

- IC Packages are becoming more complex
- Multiple component are stacked
- 3-D ICs taking it to next level
- Hard to target inner layers (ex. Memory)



Source: https://regmedia.co.uk

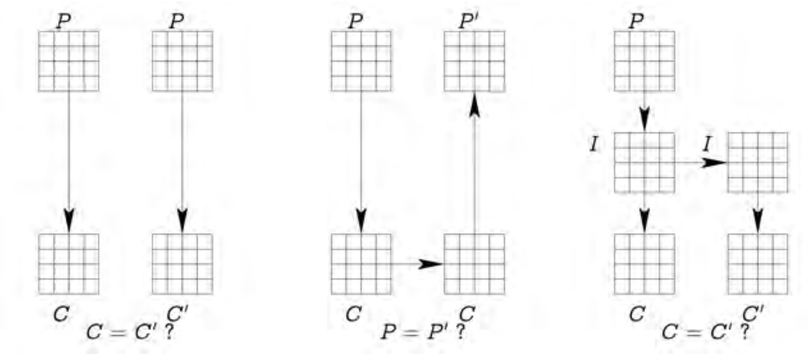
Error Detection

- **Principle:** Application of error detection codes
- Widely studied and used in communications
- Ensures data integrity
- Basic example is parity
- Generally applied on linear operations
- Can have significant overheads

Redundancy

- **Principle:** Repeat and compare
- Several variants: Compute twice, Compute forward and inverse etc.
- Equivalent to duplication in space or time
- Software duplicates in time
- Hardware can duplicate in space or time
- Compute forward and inverse shows more robustness
- At least $2\times$ overhead

Redundancy

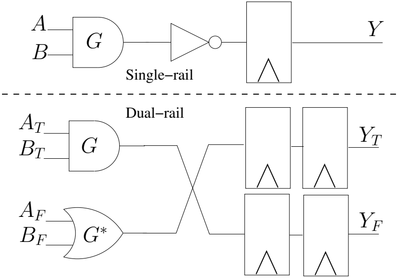


Redundancy For Fault Detection

Source: Lomne et al. : Fault Attacks and Countermeasures: A Survey

Special Logic Style

- Special representation of data to balance power consumption (ex. WDDL, BCDL)
- Introduced for side-channel protection
- Shown to have fault resistance by Selmane et al.
- High overheads



A Basic WDDL Gate with Fault Resistance

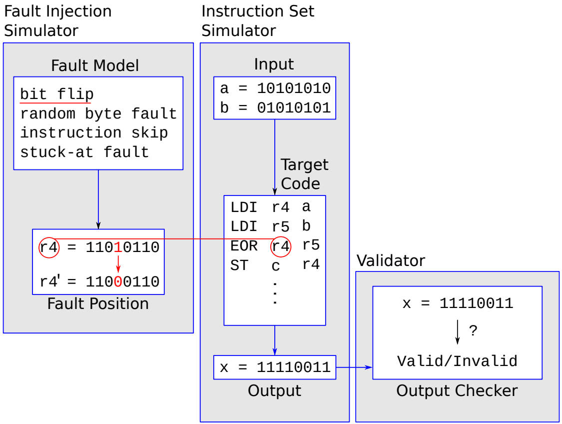
Source: Selmane et al. WDDL is Protected Against Setup Time Violation Attacks. FDTC 2010

Software Encoding Protection

- Information redundancy at software level
- Equivalent of special logic styles in software
- Data representation is modified to enable fault detection
- Some variant can also infect faults
- Initially proposed for side-channel protection
- Also demonstrate fault detection capabilities

Software Encoding Protection

- Assembly level Code Analyzer for fault resistance
- Supports several fault models.

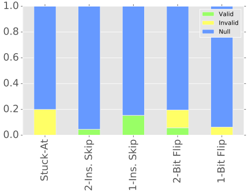


Source: Breier et al. The other side of the coin: Analyzing software encoding schemes against fault injection attacks. HOST 2016

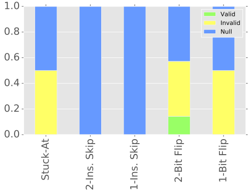
Software Encoding Protection

	Static			Device-Specific
	Encoding		DPL	
Fault model	*XOR*	*LUT*	*XOR*	*XOR*
Single bit flip	No	No	No	Yes
Double bit flip	Yes	Yes	Yes	Yes
Single instruction skip	No	No	Yes	Yes
Double instruction skip	Yes	No	Yes	Yes
Stuck-at fault	Yes	No	No	No

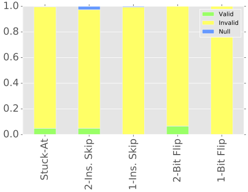
Software Encoding Protection



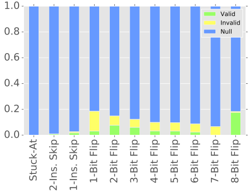
Static DPL XOR



Static Encoding LUT

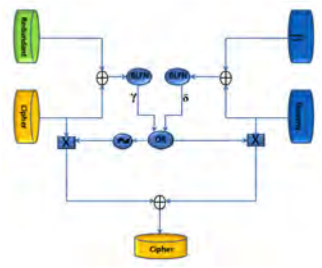


Static Encoding XOR



Device Specific XOR

Infection



- **Principle:** Tamper faulty value
- It prevents attacker from exploiting the fault
- Similar to repeat and compare scheme
- Faulty value is further diffused or randomised.
- At least $2\times$ overhead

Control Flow

- **Principle:** Verify the code execution sequence
- Applies to microcontrollers
- Modern microcontrollers can verify if the code was properly executed
- Verification of executed code signature against precomputed signature
- Cryptographic hash is a popular candidate for signature generation
- Overhead in terms of signature omputation and comparison
- If the target code is small, hashing can have big overheads
- Simpler signature schemes are then desired

Randomization

- **Principle:** Randomization reduces precision
- Most fault injection requires precise timing
- Timing randomization reduces attack precision and strenthens detection
- Jitter, dummy operations, shuffling are common techniques

Conclusion

- Fault attacks are powerful branch of physical attacks
- The techniques vary in precision and cost
- Voltage and clock based are commonly used low-cost techniques
- Laser is most precise but needs high cost and expertise
- EM is a new and interesting alternative
- Faults can be combined with other physical attacks
- A range of countermeasures was presented
- Generally a combination is required to ensure high security

Thank you!

Any questions?